IN THE CLAIMS

Please amend the claims as follows:

Claims 1-16 (Cancelled).

Claim 17 (New): An encryption/decryption apparatus comprising:

a plurality of encryption function portions provided in parallel and configured to output cipher text data by encrypting plain text data based on key data for at least one first block of data and to output plain text data by decrypting cipher text data based on key data for at least one second block of data; and

a plurality of means for generating a plurality of key data, including a first means for generating and a second means for generating, the first means for generating a plurality of key data by converting a common key using an intermediate processing result of a corresponding encryption function portion and a first type of conversion processing and the second means for generating a plurality of key data by converting the common key using an intermediate processing result of a corresponding encryption function portion and a second type of conversion processing, wherein the first type of conversion processing is different from the second type of conversion processing, and

wherein the plurality of key data generated by the first and second means for generating is input into an adjacent encryption function portion that has not begun processing.

Claim 18 (New): The encryption/decryption apparatus according to claim 17, wherein the first type of conversion processing converts the common key based on a first variable data and the second type of conversion processing converts the common key based on a second variable data, and the first variable data is different from the second variable data.

Claim 19 (New): An encryption/decryption apparatus comprising:

a plurality of encryption function portions provided in parallel and configured to output cipher text data by encrypting plain text data based on key data for at least one first block of data and to output plain text data by decrypting cipher text data based on key data for at least one second block of data; and

a plurality of key data generation portions configured to generate a plurality of key data, respectively, and including a first key generation portion and a second key generation portion, the first key generation portion being configured to generate a plurality of key data by converting a common key using an intermediate processing result of a corresponding encryption function portion and a first type of conversion processing and the second key generation portion being configured to generate a plurality of key data by converting the common key using an intermediate processing result of a corresponding encryption function portion and a second type of conversion processing,

wherein the first type of conversion processing is different from the second type of conversion processing, and

wherein the plurality of key data generated by the first and second key data generation portions is input into an adjacent encryption function portion that has not begun processing.

Claim 20 (New): The encryption/decryption apparatus according to claim 19, wherein the first type of conversion processing converts the common key based on a first variable data and the second type of conversion processing converts the common key based on a second variable data, and the first variable data is different from the second variable data.

Claim 21 (New): An authenticating apparatus for generating an authenticator from a message and authenticating said message based on the authenticator, the authenticating apparatus comprising:

a plurality of encryption function portions provided in parallel and configured to output cipher text data by encrypting plain text data based on key data for at least one first block of data and to output plain text data by decrypting cipher text data based on key data for at least one second block of data;

a plurality of means for generating a plurality of key data, including a first means for generating and a second means for generating, the first means for generating a plurality of key data by converting a common key using an intermediate processing result of a corresponding encryption function portion and a first type of conversion processing and the second means for generating a plurality of key data by converting the common key using an intermediate processing result of a corresponding encryption function portion and a second type of conversion processing,

wherein the first type of conversion processing is different from the second type of conversion processing,

wherein the plurality of key data generated by the first and second means for generating is input into an adjacent encryption function portion that has not begun processing; and

an authenticator generation portion configured to generate the authenticator based on cipher text data generated by an encryption function portion at a last stage.

Claim 22 (New): The authenticating apparatus according to claim 21, wherein the first type of conversion processing converts the common key based on a first variable data

and the second type of conversion processing converts the common key based on a second variable data, and the first variable data is different from the second variable data.

Claim 23 (New): An authenticating apparatus for generating an authenticator from a message and authenticating the message based on the authenticator, the authenticating apparatus comprising:

a plurality of encryption function portions provided in parallel and configured to output cipher text data by encrypting plain text data based on key data for at least one first block of data and to output plain text data by decrypting cipher text data based on key data for at least one second block of data;

a plurality of key data generation portions configured to generate a plurality of key data, respectively, and including a first key generation portion and a second key generation portion, the first key generation portion being configured to generate a plurality of key data by converting a common key using an intermediate processing result of a corresponding encryption function portion and a first type of conversion processing and the second key generation portion being configured to generate a plurality of key data by converting the common key using an intermediate processing result of a corresponding encryption function portion and a second type of conversion processing,

wherein the first type of conversion processing is different from the second type of conversion processing,

wherein the plurality of key data generated by the first and second key data generation portions is input into an adjacent encryption function portion that has not begun processing; and

an authenticator generation portion which generates the authenticator based on cipher text data generated by an encryption function portion at a last stage.

Claim 24 (New): The authenticating apparatus according to claim 23, wherein the first type of conversion processing converts the common key based on a first variable data and the second type of conversion processing converts the common key based on a second variable data, and the first variable data is different from the second variable data.

Claim 25 (New): A computer program stored in a computer readable storage medium used in an encryption/decryption apparatus, the computer program comprising:

a first program code which causes a computer to sequentially execute a plurality of types of encryption function processing to output cipher text data by encrypting plain text data based on key data for at least one first block of data and to output plain text data by decrypting cipher text data based on key data for at least one second block of data; and

a second program code which causes said computer to sequentially execute a plurality of types of key data generation processing, including a first type of key data generation processing and a second type of key data generation processing,

wherein the first type of key data generation processing and the second type of key data generation processing each generate a plurality of key data,

wherein the first type of key data generation processing comprises,

generating a first key data by converting a common key based on an intermediate processing result of a corresponding encryption function processing and at least a first type of conversion processing,

wherein the second type of key data generation processing comprises,

generating a second key data by converting the common key based on an intermediate processing result of a corresponding encryption processing and at least a second type of conversion processing,

wherein the first type of conversion processing is different from the second type of conversion processing, and

inputting at least one of the first and second key data to a subsequent encryption function processing that has not begun processing.

Claim 26 (New): The computer program according to claim 25, wherein the first type of conversion processing converts the common key based on a first variable data and the second conversion processing converts the common key based on a second variable data, and the first variable data is different from the second variable data.

Claim 27 (New): An encryption/decryption method comprising:

outputting cipher text data by subjecting plain text data to encryption processing based on key data in accordance with blocks of data in parallel;

outputting plain text data by subjecting cipher text data to decryption processing based on key data in accordance with blocks of data in parallel;

generating a plurality of key data including at least a first key data, wherein the first key data is generated by converting a common key based on an intermediate processing result of either encryption processing or decryption processing on a preceding stage and at least a first type of conversion processing, the first type of conversion processing being different from a second type of conversion processing used to convert the common key to generate at least a second key data; and

inputting the at least a first key data to encryption processing or decryption processing in a subsequent stage.

Claim 28 (New): The authenticating method according to claim 27, wherein the common key is converted based on at least one of a first variable data and a second variable data, wherein the first variable data is different from the second variable data.

Claim 29 (New): A computer program which generates an authenticator from a message and is stored in a computer readable storage medium used in an authenticating apparatus for authenticating the message based on the authenticator, the computer program comprising:

a first program code for causing the computer to sequentially execute a plurality of types of key data generating processing, including a first type of key data generation processing and a second type of key data generation processing,

wherein the first type of key data generation processing and the second type of key data generation processing each generate a plurality of key data,

wherein the first type of key data generation processing comprises,

generating a first key data by converting a common key based on an intermediate processing result of a corresponding encryption function processing and at least a first type of conversion processing,

wherein the second type of key data generation processing comprises,

generating a second key data by converting the common key based on an intermediate processing result of a corresponding encryption processing and at least a second type of conversion processing,

wherein the first type of conversion processing is different from the second type of conversion processing, and

inputting at least one of the first and second key data to a subsequent encryption function processing that has not begun processing; and

a third program code which causes the computer to execute authenticator generation processing for generating the authenticator based on cipher text data generated by encryption function processing on a last stage.

Claim 30 (New): The computer program according to claim 29, wherein the first type of conversion processing converts the common key based on a first variable data and the second conversion processing converts the common key based on a second variable data, and the first variable data is different from the second variable data.

Claim 31 (New): An encryption/decryption method, comprising:

outputting cipher text data by subjecting plain text data to encryption processing based on key data in accordance with blocks of data in parallel;

outputting plain text data by subjecting cipher text data to decryption processing based on key data in accordance with blocks of data in parallel;

generating a plurality of key data including at least a first key data, wherein the first key data is generated by converting a common key based on an intermediate processing result of either encryption processing or decryption processing on a preceding stage and at least one of a first and a second type of conversion processing, the first type of conversion processing being different from the second type of conversion processing; and

inputting the at least a first key data to encryption processing or decryption processing in a subsequent stage.

Claim 32 (New): The computer program according to claim 31, wherein the first type of conversion processing converts the common key based on a first variable data and the

second conversion processing converts the common key based on a second variable data, and the first variable data is different from the second variable data.

Claim 33 (New): The encryption/decryption apparatus according to claim 17, wherein the first type of conversion processing converts the common key based on a first function and the second type of conversion processing converts the common key based on a second function, and the first function is different from the second function.

Claim 34 (New): The encryption/decryption apparatus according to claim 17, wherein the first type of conversion processing and the second type of conversion processing each convert the common key based on a function, and the first type of conversion processing acts on at least a first bit position and the second type of conversion processing acts on at least a second bit position different from the at least one first bit position.

Claim 35 (New): The encryption/decryption apparatus according to claim 19, wherein the first type of conversion processing converts the common key based on a first function and the second type of conversion processing converts the common key based on a second function, and the first function is different from the second function.

Claim 36 (New): The encryption/decryption apparatus according to claim 19, wherein the first type of conversion processing and the second type of conversion processing each convert the common key based on a function, and the first type of conversion processing acts on at least a first bit position and the second type of conversion processing acts on at least a second bit position different from the at least one first bit position.

Claim 37 (New): The authenticating apparatus according to claim 21, wherein the first type of conversion processing converts the common key based on a first function and the second type of conversion processing converts the common key based on a second function, and the first function is different from the second function.

Claim 38 (New): The authenticating apparatus according to claim 21, wherein the first type of conversion processing and the second type of conversion processing each convert the common key based on a function, and the first type of conversion processing acts on at least a first bit position and the second type of conversion processing acts on at least a second bit position different from the at least one first bit position.

Claim 39 (New): The authenticating apparatus according to claim 23, wherein the first type of conversion processing converts the common key based on a first function and the second type of conversion processing converts the common key based on a second function, and the first function is different from the second function.

Claim 40 (New): The authenticating apparatus according to claim 23, wherein the first type of conversion processing and the second type of conversion processing each convert the common key based on a function, and the first type of conversion processing acts on at least a first bit position and the second type of conversion processing acts on at least a second bit position different from the at least one first bit position.

Claim 41 (New): The computer program according to claim 25, wherein the first type of conversion processing converts the common key based on a first function and the second

type of conversion processing converts the common key based on a second function, and the first function is different from the second function.

Claim 42 (New): The computer program according to claim 25, wherein the first type of conversion processing and the second type of conversion processing each convert the common key based on a function, and the first type of conversion processing acts on at least a first bit position and the second type of conversion processing acts on at least a second bit position different from the at least one first bit position.

Claim 43 (New): The computer program according to claim 27, wherein the first type of conversion processing converts the common key based on a first function and the second type of conversion processing converts the common key based on a second function, and the first function is different from the second function.

Claim 44 (New): The computer program according to claim 27, wherein the first type of conversion processing and the second type of conversion processing each convert the common key based on a function, and the first type of conversion processing acts on at least a first bit position and the second type of conversion processing acts on at least a second bit position different from the at least one first bit position.

Claim 45 (New): The encryption/decryption method according to claim 29, wherein the first type of conversion processing converts the common key based on a first function and the second type of conversion processing converts the common key based on a second function, and the first function is different from the second function.

Claim 46 (New): The encryption/decryption method according to claim 29, wherein the first type of conversion processing and the second type of conversion processing each convert the common key based on a function, and the first type of conversion processing acts on at least a first bit position and the second type of conversion processing acts on at least a second bit position different from the at least one first bit position.

Claim 47 (New): The encryption/decryption method according to claim 31, wherein the first type of conversion processing converts the common key based on a first function and the second type of conversion processing converts the common key based on a second function, and the first function is different from the second function.

Claim 48 (New): The encryption/decryption method according to claim 31, wherein the first type of conversion processing and the second type of conversion processing each convert the common key based on a function, and the first type of conversion processing acts on at least a first bit position and the second type of conversion processing acts on at least a second bit position different from the at least one first bit position.

Claim 49 (New): The encryption/decryption apparatus according to claim 17, wherein the at least one first block of data is the at least one second block of data.

Claim 50 (New): The encryption/decryption apparatus according to claim 19, wherein the at least one first block of data is the at least one second block of data.

Claim 51 (New): The authenticating apparatus according to claim 21, wherein the at least one first block of data is the at least one second block of data.

Claim 52 (New): The authenticating apparatus according to claim 23, wherein the at least one first block of data is the at least one second block of data.

Claim 53 (New): The computer program according to claim 25, wherein the at least one first block of data is the at least one second block of data.